INTERFERENCE SEARCH

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	1	(encrypt$3 licens$3 decrypt$3 key attribute public private sign$3 authoriz$3).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/01 20:14
L3	4	(encrypt$3 licens$3 decrypt$3 key attribute public private signature).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/01 20:14
L4	5	(encrypt$3 licens$3 decrypt$3 key attribute public private hash).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/01 20:14
L5	1	(encrypt$3 licens$3 decrypt$3 key attribute public private hash network).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/01 20:14
L6	6	(encrypt$3 licens$3 decrypt$3 key attribute public private network).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	AND	ON	2007/03/01 20:14

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	199	(380/285).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/01 17:54
S2	149	S1 and @ad<"20010706"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/01 18:55
S6	6809	((380/282) or (380/259) or (380/203) or (713/193) or (713/167) or (713/165) or (713/194) or (713/171) or (705/59) or (380/29) or (380/42) or (380/277) or (726/1)).CCLS.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/01 18:55
S7	3403	S6 and @ad<"20010706"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/01 19:00
S8	90	S7 and licens$3 and attributes and (public adj key) and decrypt$3 and (private adj key)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/01 18:58
S9	662	(digital$2 adj (sign$3 or signature)) same hash$3 same decrypt$3 same compar$5	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/01 19:00
S10	253	S9 and @ad<"20010706"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/01 19:04
S11	0	licens$3 same (decryption adj key) same (public adj key) same encrypt$3 same (digital$2 adj (sign$3 or signature)) and ((cell$3 or mobile) adj phone)	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/01 19:04
S12	20	licens$3 same (decryption adj key) same (public adj key) same encrypt$3 same (digital$2 adj (sign$3 or signature))	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/01 19:04

EAST Search History

S13	9	S12 and @ad<"20010706"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/01 19:04

Terms used **public key** and **private key** and **license** and **attributes** and **encrypt$3** and **decrypt$3** and **signature**

Found **1,490** of **198,146**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

☐ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Multi-agent systems and social behavior: A user-centric anonymous authorisation framework in e-commerce environment

Richard Au, Harikrishna Vasanta, Kim-Kwang Raymond Choo, Mark Looi

March 2004 **Proceedings of the 6th international conference on Electronic commerce ICEC '04**

Publisher: ACM Press

Full text available: pdf(291.06 KB) Additional Information: full citation, abstract, references, citings

A novel user-centric authorisation framework suitable for e-commerce in an open environment is proposed. The credential-based approach allows a user to gain access rights anonymously from various service providers who may not have pre-existing relationships. Trust establishment is achieved by making use of referrals from external third parties in the form of *Anonymous Attribute Certificates.* The concepts of *One-task Authorisation Key* and *Binding Signature* are proposed to fac ...

2 Authentication and signature schemes: On the performance, feasibility, and use of forward-secure signatures

Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel

October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**

Publisher: ACM Press

Full text available: pdf(386.51 KB) Additional Information: full citation, abstract, references, citings, index terms

Forward-secure signatures (FSSs) have recently received much attention from the cryptographic theory community as a potentially realistic way to mitigate many of the difficulties digital signatures face with key exposure. However, no previous works have explored the practical performance of these proposed constructions in real-world applications, nor have they compared FSS to traditional, non-forward-secure, signatures in a non-asymptotic way.We present an empirical evaluation of several FSS sch ...

Keywords: digital signatures, forward-secure signatures

3 DRM experience: Digital rights management in a 3G mobile phone and beyond

Thomas S. Messerges, Ezzat A. Dabbish

October 2003 **Proceedings of the 3rd ACM workshop on Digital rights management**

DRM '03
Publisher: ACM Press

Full text available: pdf(306.59 KB) Additional Information: full citation, abstract, references, citings, index terms

In this paper we examine how copyright protection of digital items can be securely managed in a 3G mobile phone and other devices. First, the basic concepts, strategies, and requirements for digital rights management are reviewed. Next, a framework for protecting digital content in the embedded environment of a mobile phone is proposed and the elements in this system are defined. The means to enforce security in this system are described and a novel "Family Domain" approach to content management ...

Keywords: MPEG-21, copyright protection, cryptography, digital content, digital rights management, embedded system, key management, mobile phone, open mobile alliance, security

4 Technologies for repository interoperation and access control

Shirley Browne, Jack Dongarra, Jeff Horner, Paul McMahan, Scott Wells
May 1998 **Proceedings of the third ACM conference on Digital libraries DL '98**
Publisher: ACM Press
Full text available: pdf(1.14 MB) Additional Information: full citation, references, citings, index terms

5 Mobile computing and applications (MCA): Delivering Attribute Certificates over GPRS

Georgios Kambourakis, Angelos Rouskas, Stefanos Gritzalis
March 2004 **Proceedings of the 2004 ACM symposium on Applied computing SAC '04**
Publisher: ACM Press
Full text available: pdf(182.76 KB) Additional Information: full citation, abstract, references, index terms

Attribute Certificates (ACs) have been developed and standardized by the ANSI X9 committee as an alternative and better approach, to X.509 public key certificates, for carrying authorization information. Attribute Authorities (AA) bind the characteristics of an entity (called attributes) to that entity by signing the appropriate AC. Therefore, ACs can be used for controlling access to system resources and employing role-based authorization and access controls policies accordingly. Although ACs a ...

Keywords: GPRS, PKI, UMTS, attribute certificates, performance evaluation

6 Some facets of complexity theory and cryptography: A five-lecture tutorial

Jörg Rothe
December 2002 **ACM Computing Surveys (CSUR)**, Volume 34 Issue 4
Publisher: ACM Press
Full text available: pdf(2.78 MB) Additional Information: full citation, abstract, references, citings, index terms, review

In this tutorial, selected topics of cryptology and of computational complexity theory are presented. We give a brief overview of the history and the foundations of classical cryptography, and then move on to modern public-key cryptography. Particular attention is paid to cryptographic protocols and the problem of constructing key components of protocols such as one-way functions. A function is one-way if it is easy to compute, but hard to invert. We discuss the notion of one-way functions both ...

Keywords: Complexity theory, interactive proof systems, one-way functions, public-key

cryptography, zero-knowledge protocols

7 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5
Publisher: ACM Press

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

8 Data protection: Secure attribute-based systems

Matthew Pirretti, Patrick Traynor, Patrick McDaniel, Brent Waters
October 2006 **Proceedings of the 13th ACM conference on Computer and communications security CCS '06**
Publisher: ACM Press

Full text available: pdf(1.13 MB) Additional Information: full citation, abstract, references, citings, index terms

Attributes define, classify, or annotate the datum to which they are assigned. However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. In this paper, we introduce a novel secure information management architecture based on emerging attribute-based encryption (ABE) primitives. A policy system that meets the needs of complex policies is defined and illustrated. Based on the needs of those polic ...

Keywords: applied cryptography, attribute-based encryption, secure systems

9 A security architecture for fault-tolerant systems

Michael K. Reiter, Kenneth P. Birman, Robbert van Renesse
November 1994 **ACM Transactions on Computer Systems (TOCS)**, Volume 12 Issue 4
Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Process groups are a common abstraction for fault-tolerant computing in distributed systems. We present a security architecture that extends the process group into a security abstraction. Integral parts of this architecture are services that securely and fault tolerantly support cryptographic key distribution. Using replication only when necessary, and introducing novel replication techniques when it was necessary, we have constructed these services both to be easily defensible against atta ...

Keywords: key distribution, multicast, process groups

10 Credentials: Concealing complex policies with hidden credentials

Robert W. Bradshaw, Jason E. Holt, Kent E. Seamons
October 2004 **Proceedings of the 11th ACM conference on Computer and**

communications security CCS '04

Publisher: ACM Press

Full text available: pdf(219.13 KB) Additional Information: full citation, abstract, references, citings, index terms

Hidden credentials are useful in protecting sensitive resource requests, resources, policies, and credentials. We propose a significant performance improvement when implementing hidden credentials using Boneh/Franklin Identity Based Encryption. We also propose a substantially improved secret splitting scheme for enforcing complex policies, and show how it improves concealment of policies from nonsatisfying recipients.

Keywords: authentication, credentials, identity based encryption, privacy, secret sharing, trust negotiation

11 Verification and security: Policy-hiding access control in open environment

Jiangtao Li, Ninghui Li

July 2005 **Proceedings of the twenty-fourth annual ACM symposium on Principles of distributed computing PODC '05**

Publisher: ACM Press

Full text available: pdf(247.72 KB) Additional Information: full citation, abstract, references, citings, index terms

In trust management and attribute-based access control systems, access control decisions are based on the attributes (rather than the identity) of the requester: Access is granted if Alice's attributes in her certificates satisfy Bob's access control policy. In this paper, we develop a policy-hiding access control scheme that protects both sensitive attributes and sensitive policies. That is, Bob can decide whether Alice's certified attribute values satisfy Bob's policy, without Bob learning any ...

Keywords: access control, automated trust negotiation, cryptographic commitment, cryptographic protocol, digital credentials, evaluation, privacy, secure function

12 Cryptographic protocols: Design and implementation of the *idemix* anonymous credential system

Jan Camenisch, Els Van Herreweghen

November 2002 **Proceedings of the 9th ACM conference on Computer and communications security CCS '02**

Publisher: ACM Press

Full text available: pdf(1.09 MB) Additional Information: full citation, abstract, references, citings, index terms

Anonymous credential systems [8, 9, 12, 24] allow anonymous yet authenticated and accountable transactions between users and service providers. As such, they represent a powerful technique for protecting users' privacy when conducting Internet transactions. In this paper, we describe the design and implementation of an anonymous credential system based on the protocols developed by [6]. The system is based on new high-level primitives and interfaces allowing for easy integration into access cont ...

Keywords: anonymous credential systems, cryptographic protocols, privacy

13 Authentication metric analysis and design

Michael K. Reiter, Stuart G. Stubblebine

May 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 2
Publisher: ACM Press

Full text available: pdf(154.45 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Authentication using a path of trusted intermediaries, each able to authenicate the next in the path, is a well-known technique for authenicating entities in a large-scale system. Recent work has extended this technique to include multiple paths in an effort to bolster authentication, but the success of this approach may be unclear in the face of intersecting paths, ambiguities in the meaning of certificates, and interdependencies in the use of different keys. Thus, several authors have pro ...

Keywords: metrics of authentication, public key infrastructure

14 Email and security: How to make secure email easier to use

Simson L. Garfinkel, David Margrave, Jeffrey I. Schiller, Erik Nordlander, Robert C. Miller
April 2005 **Proceedings of the SIGCHI conference on Human factors in computing systems CHI '05**
Publisher: ACM Press

Full text available: pdf(419.10 KB) Additional Information: full citation, abstract, references, citings, index terms

Cryptographically protected email has a justly deserved reputation of being difficult to use. Based on an analysis of the PEM, PGP and S/MIME standards and a survey of 470 merchants who sell products on Amazon.com, we argue that the vast majority of Internet users can start enjoying digitally signed email today. We present suggestions for the use of digitally signed mail in e-commerce and simple modifications to webmail systems that would significantly increase integrity, privacy and authorship ...

Keywords: e-commerce, user interaction design, user studies

15 Trust management: Preventing attribute information leakage in automated trust negotiation

Keith Irwin, Ting Yu
November 2005 **Proceedings of the 12th ACM conference on Computer and communications security CCS '05**
Publisher: ACM Press

Full text available: pdf(217.27 KB) Additional Information: full citation, abstract, references, index terms

Automated trust negotiation is an approach which establishes trust between strangers through the bilateral, iterative disclosure of digital credentials. Sensitive credentials are protected by access control policies which may also be communicated to the other party. Ideally, sensitive information should not be known by others unless its access control policy has been satisfied. However, due to bilateral information exchange, information may flow to others in a variety of forms, many of which can ...

Keywords: attribute-based access control, privacy, trust negotiation

16 DRM usability and legal issues: Import/export in digital rights management

Reihaneh Safavi-Naini, Nicholas Paul Sheppard, Takeyuki Uehara
October 2004 **Proceedings of the 4th ACM workshop on Digital rights management DRM '04**
Publisher: ACM Press

Additional Information:

Full text available: pdf(211.60 KB) full citation, abstract, references, citings, index terms

The inherently controlled nature of digital rights management systems does little to promote inter-operability of systems provided by different vendors. In this paper, we consider import and export functionality by which multimedia protected by one digital rights management regime can be made available to a multimedia device that supports a different digital rights management regime, without compromising the protection afforded to the content under the original regime. We first identify speci ...

Keywords: digital rights management, export, import, inter-operability

17 Digital signatures: can they be accepted as legal signatures in EDI?

Patrick W. Brown
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press

Full text available: pdf(809.34 KB) Additional Information: full citation, abstract, references, citings, index terms

Digital Signature (DS) technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as those developed for handwritten signatures on paper. Digital signature technology promises assurance at least equal to written signatures. From a legal standpoint, this assurance remains to be tested in the evidentiary process. Business policies for organizational use of this technology ar ...

Keywords: EDI, cryptography, digital signatures, distributed systems, law

18 Safety in automated trust negotiation

William H. Winsborough, Ninghui Li
August 2006 **ACM Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 3
Publisher: ACM Press
Full text available: pdf(383.26 KB) Additional Information: full citation, abstract, references, index terms

Exchange of attribute credentials is a means to establish mutual trust between strangers wishing to share resources or conduct business transactions. Automated Trust Negotiation (ATN) is an approach to regulate the exchange of sensitive information during this process. It treats credentials as potentially sensitive resources, access to which is under policy control. Negotiations that correctly enforce policies have been called "safe" in the literature. Prior work on ATN lacks an adeq ...

Keywords: Access control, attribute-based access control, automated trust negotiation, credentials, safety, strategy

19 The emerging law of international electronic commerce: recent work by UNCITRAL

Henry Deeb Gabriel
September 2003 **Proceedings of the 5th international conference on Electronic commerce ICEC '03**
Publisher: ACM Press
Full text available: pdf(148.85 KB) Additional Information: full citation, abstract, references, index terms

This paper describes the minimal aspects of any law intended to govern electronic commerce, and discusses the recent attempts by the United Nations Commission on

International Trade Law to create a legal framework for electronic commerce. Electronic commerce laws recognize the validity of electronic records, signatures and contracts without changing the underlying substantive law of contracts. The UNCITRAL approach to electronic commerce legislation is based on the "functional-equivalent" approa ...

Keywords: contract, functional equivalence, media neutrality

20 APL.NET encryption HOWTO

Vladimir Kutinsky
March 2004 **ACM SIGAPL APL Quote Quad**, Volume 34 Issue 2
Publisher: ACM Press
Full text available: pdf(233.13 KB) Additional Information: full citation, abstract, references

The article outlines the key points of building a Dyalog APL interface to the GNU Privacy Guard (GnuPG), a tool for cryptographic privacy and authentication. The main purpose of the interface is to use the GnuPG's functionality to encrypt data and create digital signatures directly from APL programs. The article briefly describes .NET classes that form the core of the interface and provide effective means to manage processes running on a computer. It also contains a number of examples demonstrat ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next